UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/071,228	02/08/2002	Steven A. Pettit	ENB-012RCE2	9237

959 7590 06/11/2008

LAHIVE & COCKFIELD, LLP
ONE POST OFFICE SQUARE
BOSTON, MA 02109

EXAMINER	
WONG, WARNER	
ART UNIT	PAPER NUMBER
2616	

MAIL DATE	DELIVERY MODE
06/11/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/071,228	PETTIT ET AL.	
	Examiner	Art Unit	
	WARNER WONG	2616	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 March 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,5,7-9,11,13-15,17,19-21,23,26-29,31,33-35,37 and 40* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,5,7-9,11,13-15,17,19-21,23,26-29,31,33-35,37 and 40* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. Claims 1-3, 5 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over See (US 2003/0021283) in view of Curie (US 6,871,232) and Ji (US 7,227,842).

Regarding claim 1, See describes a distributed network management system of controlling usage of network resources on a communication network (abstract, individual network device each distributively performing rules/policy management), comprising:

(a) creating one or more packet rules (policy rules) for analyzing packets received at one or more devices of the communications network, each rule including a condition and action to be taken if a packet received at a device satisfies the condition (fig. 4 and paragraph 35);

(b) storing the one or more packet rules (paragraph 35, policy rules stored in repository table);

(c) creating one or more service abstractions (policy groups), each service abstraction representing a [named] set of one or more of the packet rules (paragraph 35, "According to one embodiment, the policy rules are organized into policy groups based on a rule type 52";

(d) storing the one or more service abstractions (paragraph 35, policy groups stored in repository table);

(e) associating one or more of the service abstractions with a computer host of the communications network (paragraph 27, where network devices may be computer hosts, and paragraph 30, "According to one embodiment, the policies relevant to a particular network device 24, 26, 28 are selected based on a role assigned to the device" and paragraph 35, "A rule type may organize policies into role policies").

See fails to describe:

controlling usage based on the identity of an authenticated user, and associating one or more service abstraction with an authenticated user to control network resource usage by the authenticated user.

Curie describes:

controlling usage based on the identity of an authenticated user, and associating one or more service abstraction with an authenticated user to control network resource usage by the authenticated user (abstract, fig. 11A, col. 11, lines 50-52 & col. 17, lines 16-18, user authentication, plus col. 21, lines 50-65, associating/grouping common policy (abstraction) with the user so that the user can use the network resources).

It would have been obvious to one with ordinary skill in the art at the time of invention by applicant to describe an authenticated user is used for controlling network usage and is associated with an service abstraction as described in Curie for the network usage control of See.

The motivation for combining the teachings is that it enables the resource provisioning of plurality of organizations (with different users) using a single, centralized logical server (Curie, col. 3, lines 41-57).

Curie further describes the compatible means of creating service abstractions in response to a user (col. 1, lines 52-60, in response to a new user, setting up the resources of such role).

See and Curie combined fail to explicitly describe:

wherein one or more packet rules are defined to examine any portion of a packet.

Ji describes packet classification comprising:

wherein one or more packet rules are defined to examine any portion of a packet (abstract, employs bitmaps to classify any field (portion) of an incoming packet).

Ji also describes manually (in response to a user) setting up rules (col. 15, lines 35-38).

It would have been obvious to one with ordinary skill in the art at the time of invention by application to modify the packet classification of See and Curie combined such that the packet rules can examine any portion of a packet as in Ji.

The motivation for combining the teachings is that it results in a high performance packet classification solution that provides an optimal tradeoff between performance and memory size (Ji, col. 4, lines 20-22).

Regarding claim 2, See describes all limitations set forth in claim 1. See further describes:

(f) configuring a network device of the communications network with one or more packet rules according to at least one of the service abstractions (policy groups) (paragraph 26, "The policy repository 22 stores a plurality of policy rules that may be used by the network devices 24, 26, 28 to control different network elements" and paragraph 38, "The action 58 may be identifying a policy group based on a device attribute..")

Regarding claim 3, See describes all limitations set forth in claim 2. See further describes:

configuring a port module of a switching device of the communications network with one or more packet rules according to at least one of the service abstractions (paragraph 22, "According to one embodiment, the network policies are used to .. disable network ports based on predetermined conditions,")

Regarding claim 5, See describes all limitations set forth in claim 1. See further describes:

(C) distributing the one or more service abstractions to one or more network devices residing on the communications network (paragraph 30, "According to one embodiment, the policies relevant to a particular network device 24, 26, 28 are selected based on a role assigned to the device" and paragraph 35, "A rule type may organize policies into role policies").

Regarding claim 26, See describes a system of controlling usage of network resources on a communication network (abstract, individual network device each distributively performing rules/policy management), comprising:

(a) creating one or more packet rules (policy rules) for analyzing packets received at one or more devices of the communications network, each rule including a condition and action to be taken if a packet received at a device satisfies the condition (fig. 4 and paragraph 35);

(b) storing the one or more packet rules (paragraph 35, policy rules stored in repository table);

(c) creating one or more service abstractions (policy groups), each service abstraction representing a named set of one or more of the packet rules (paragraph 35, "According to one embodiment, the policy rules are organized into policy groups based on a rule type 52".

(d) storing the one or more service abstractions (paragraph 35, policy groups stored in repository table);

See lacks describing a computer program product to perform the above-mentioned system, comprising:

a computer readable medium and computer readable signals stored on the computer readable medium that define instructions that, as a result of being executed by a computer, instruct the computer to perform the process.

The examiner takes official notice that the system of See may be implemented using a computer comprising a readable medium and a program with instructions which executes the process. The motivation being that such implementation using a [generic] computer may be more economical and faster to develop than via a customized hardware system.

See fails to describe:

controlling usage based on the identity of an authenticated user, and associating one or more service abstraction with an authenticated user.

Curie describes:

controlling usage based on the identity of an authenticated user, and associating one or more service abstraction with an authenticated user to control network resource usage by the authenticated user (abstract, fig. 11A, col. 11, lines 50-52 & col. 17, lines 16-18, user authentication, plus col. 21, lines 50-65, associating/grouping common policy (abstraction) with the user so that the user can use the network resources).

It would have been obvious to one with ordinary skill in the art at the time of invention by applicant to describe an authenticated user is used for controlling network usage and is associated with an service abstraction as described in Curie for the network usage control of See.

The motivation for combining the teachings is that it enables the resource provisioning of plurality of organizations (with different users) using a single, centralized logical server (Curie, col. 3, lines 41-57).

Curie further describes the compatible means of creating service abstractions in response to a user (col. 1, lines 52-60, in response to a new user, setting up the resources of such role).

See and Curie combined fail to explicitly describe:

wherein one or more packet rules are defined to examine any portion of a packet.

Ji describes packet classification comprising:

wherein one or more packet rules are defined to examine any portion of a packet (abstract, employs bitmaps to classify any field (portion) of an incoming packet).

Ji also describes manually (in response to a user) setting up rules (col. 15, lines 35-38).

It would have been obvious to one with ordinary skill in the art at the time of invention by application to modify the packet classification of See and Curie combined such that the packet rules can examine any portion of a packet as in Ji.

The motivation for combining the teachings is that it results in a high performance packet classification solution that provides an optimal tradeoff between performance and memory size (Ji, col. 4, lines 20-22).

2. Claim 7-9, and 11, 27-29 and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over See in view of Curie and Ji, and further in view of Azarmi (5,905,715).

Regarding claim 7, See, Curie and Ji combined describe all limitations set forth in claim 1, where the user is an authenticated user (Curie, col. 17, lines 16-18).

See, Curie and Ji combined lack what Azarmi describes:

(f) creating one or more role abstractions (feature-describing data set), each role abstraction representing a role of a user with respect to the communications network (manageable aspect of the communications network), and each role abstraction including a set of one more service abstractions (management rule profiles) (col. 2, lines 42-51, & fig. 20 where such control/provisioning is for [associated with] individual users).

It would have been obvious to one with ordinary skill in the art at the time of invention by applicant to specify (another) role abstraction layer to group the (existing) service abstraction layer. The motivation being that "It defines a structural architecture within which business processes, and therefore management systems required to provide services on a network", Azarmi, col. 2, lines 10-12).

Regarding claim 8, See, Curie, Ji and Azarmi combined describe all limitations set forth in claim 7. See, Curie, Ji and Azarmi further describe:

(g) configuring a network device of the communications network with one or more packet rules according to one of the role abstractions (See, paragraph 26, "The policy repository 22 stores a plurality of policy rules that may be used by the network devices 24, 26, 28 to control different network elements" and See, paragraph 38, "The action 58 may be identifying a policy group based on a device attribute.." *where the policy group [i.e. service abstraction layer] is replaced by Azarmi's feature set [i.e. role abstraction layer]*).

Regarding claim 9, See, Curie, Ji and Azarmi combined describe all limitations set forth in claim 8. See, Curie, Ji and Azarmi further describe:

configuring a port module of a switching device of the communications network with one or more packet rules according to at least one of the role abstractions (See, paragraph 22, "According to one embodiment, the network policies are used to .. disable network ports based on predetermined conditions", *where the policy (group) [i.e. service abstraction layer] is replaced by Azarmi's feature set [i.e. role abstraction layer]*).

Regarding claim 11, See, Curie, Ji and Azarmi combined describe all limitations set forth in claim 7. See, Curie, Ji and Azarmi further describe:

(g) distributing the one or more role abstractions to one or more network devices residing on the communications network (See, paragraph 30, "According to one embodiment, the policies relevant to a particular network device 24, 26, 28 are selected based on a role assigned to the device" and See, paragraph 35, "A rule type may organize policies into role policies", *where the role (policy) [i.e. service abstraction layer] is replaced by Azarmi's feature set [i.e. role abstraction layer]*).

Regarding claims 27, See describes a method of controlling usage of network resources on a communication network (abstract, individual network device each distributively performing rules/policy management), comprising:

(a) defining one or more packet rules (policy rules) for analyzing packets received at one or more devices of the communication network, each rule including a condition and action to be taken if a packet received at a device satisfies the condition (fig. 4 and paragraph 35);

(b) providing the one or more packet rules (paragraph 35, packet rules in repository table ready for use);

See lacks what Azarmi describes:

(c) defining one or more role abstractions (feature-describing data set), each role abstraction representing a role of a user with respect to the communications network (manageable aspect of the communications network), and each role abstraction including a set of one more packet rule (management rule profiles containing

management rules) (col. 2, lines 42-51, & fig. 20 where such control/provisioning is for [associated with] individual users).

(d) providing the one or more role abstractions (col. 2, lines 30-34, provided for monitoring and controlling the service provisions).

It would have been obvious to one with ordinary skill in the art at the time of invention by applicant to specify the role abstraction layer to group the packet rules (layer). The motivation being that "It defines a structural architecture within which business processes, and therefore management systems required to provide services on a network", Azarmi, col. 2, lines 10-12.

See and Azarmi combined fails to describe:

controlling usage based on the identity of an authenticated user, and associating one or more service abstraction with an authenticated user.

Curie describes:

controlling usage based on the identity of an authenticated user, and associating one or more service abstraction with an authenticated user to control network resource usage by the authenticated user (abstract, fig. 11A, col. 11, lines 50-52 & col. 17, lines 16-18, user authentication, plus col. 21, lines 50-65, associating/grouping common policy (abstraction) with the user so that the user can use the network resources).

It would have been obvious to one with ordinary skill in the art at the time of invention by applicant to describe an authenticated user is used for controlling network usage and is associated with an service abstraction as described in Curie for the network usage control of See and Azarmi.

The motivation for combining the teachings is that it enables the resource provisioning of plurality of organizations (with different users) using a single, centralized logical server (Curie, col. 3, lines 41-57).

Curie further describes the compatible means of creating service abstractions in response to a user (col. 1, lines 52-60, in response to a new user, setting up the resources of such role).

See, Azarmi and Curie combined fail to explicitly describe:

wherein one or more packet rules are defined to examine any portion of a packet.

Ji describes packet classification comprising:

wherein one or more packet rules are defined to examine any portion of a packet (abstract, employs bitmaps to classify any field (portion) of an incoming packet).

Ji also describes manually (in response to a user) setting up rules (col. 15, lines 35-38).

It would have been obvious to one with ordinary skill in the art at the time of invention by application to modify the packet classification of See, Azarmi and Curie combined such that the packet rules can examine any portion of a packet as in Ji.

The motivation for combining the teachings is that it results in a high performance packet classification solution that provides an optimal tradeoff between performance and memory size (Ji, col. 4, lines 20-22).

Regarding claim 28, See, Azarmi, Curie and Ji combined describe all limitations set forth in claim 27. See, Azarmi, Curie and Ji further describe:

(e) configuring a network device of the communications network with one or more packet rules according to one of the role abstractions (See, paragraph 26, "The policy repository 22 stores a plurality of policy rules that may be used by the network devices 24, 26, 28 to control different network elements" and See, paragraph 38, "The action 58 may be identifying a policy group based on a device attribute.." *where the policy group [i.e. service abstraction layer] is replaced by Azarmi's feature set [i.e. role abstraction layer]*).

Regarding claim 29, See, Azarmi, Curie and Ji combined describe all limitations set forth in claim 28. See, Azarmi, Curie and Ji further describe step (C) of:

configuring a port module of a switching device of the communications network with one or more packet rules according to at least one of the role abstractions (See, paragraph 22, "According to one embodiment, the network policies are used to .. disable network ports based on predetermined conditions", *where the policy (group) [i.e. service abstraction layer] is replaced by Azarmi's feature set [i.e. role abstraction layer]*).

Regarding claim 31, See, Azarmi, Curie and Ji combined describe all limitations set forth in claim 27. See, Azarmi, Curie and Ji further describe step (C) of:

(e) distributing the one or more role abstractions to one or more network devices residing on the communications network (See, paragraph 30, "According to one embodiment, the policies relevant to a particular network device 24, 26, 28 are selected based on a role assigned to the device" and See, paragraph 35, "A rule type may organize policies into role policies", *where the role (policy) [i.e. service abstraction layer] is replaced by Azarmi's feature set [i.e. role abstraction layer]*).

3. Claims 13-15 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over See in view of Nessett, Curie and Ji.

Regarding claim 13, See describes a system for controlling usage of network resources on a communications network (abstract, individual network device each distributively performing rules/policy management), the system comprising:

creating one or more packet rules for analyzing packets received at one or more devices of the communications network, each rule including a condition and action to be taken if a packet received at a device satisfies the condition; and

creating one or more service abstractions, each service abstraction representing a named set of one or more of the packet rules.

[assigning logic to] associate one or more of the service abstractions with a user (computer host) of the communications network (paragraph 27, where network devices may be computer hosts, which is a user of the communication network, and paragraph 30, "According to one embodiment, the policies relevant to a particular network device 24, 26, 28 are selected based on a role assigned to the device" and paragraph 35, "A rule type may organize policies into role policies").

storage means for storing one or more packet rules (paragraph 35, policy rules stored in repository table);

See lacks what Nessett describes:

a rule editing module [to create pack rules] (fig. 1, security policy management back-end #32) and a service editing module [means to create service abstractions] (fig. 1, security policy language interpreter #34)

It would have been obvious to one with ordinary skill in the art at the time of invention by applicant to specify respective editing modules to be used for creating the packet rules and service abstractions as specified in See. The motivation for using separate modules in performing layered rules & service abstraction functionality is "As the partitioning becomes finer grained, access to resources outside of the firewall partition experiences increasing degraded performance. Another approach to this problem is to distribute firewall functionality down into lower layers of the protocol hierarchy" (Nessett, col. 2, lines 51-56).

See and Nessett combined fail to describe:

controlling usage based on the identity of an authenticated user, and associating one or more service abstraction with an authenticated user.

Curie describes:

controlling usage based on the identity of an authenticated user, and associating one or more service abstraction with an authenticated user to control network resource usage by the authenticated user (abstract, fig. 11A, col. 11, lines 50-52 & col. 17, lines 16-18, user authentication, plus col. 21, lines 50-65, associating/grouping common policy (abstraction) with the user so that the user can use the network resources).

It would have been obvious to one with ordinary skill in the art at the time of invention by applicant to describe an authenticated user is used for controlling network

usage and is associated with an service abstraction as described in Curie for the network usage control of See and Nessett.

The motivation for combining the teachings is that it enables the resource provisioning of plurality of organizations (with different users) using a single, centralized logical server (Curie, col. 3, lines 41-57).

Curie further describes the compatible means of creating service abstractions in response to a user (col. 1, lines 52-60, in response to a new user, setting up the resources of such role).

See, Nessett and Curie combined fail to explicitly describe:

wherein one or more packet rules are defined to examine any portion of a packet.

Ji describes packet classification comprising:

wherein one or more packet rules are defined to examine any portion of a packet (abstract, employs bitmaps to classify any field (portion) of an incoming packet).

Ji also describes manually (in response to a user) setting up rules (col. 15, lines 35-38).

It would have been obvious to one with ordinary skill in the art at the time of invention by application to modify the packet classification of See and Curie combined such that the packet rules can examine any portion of a packet as in Ji.

The motivation for combining the teachings is that it results in a high performance packet classification solution that provides an optimal tradeoff between performance and memory size (Ji, col. 4, lines 20-22).

Regarding claim 14, See, Nessett, Curie and Ji combined describe all limitations set forth in claim 13. See further describes:

[logic to] configure a network device of the communications network with one or more packet rules according to at least one of the service abstractions (policy groups) (paragraph 26, "The policy repository 22 stores a plurality of policy rules that may be used by the network devices 24, 26, 28 to control different network elements" and paragraph 38, "The action 58 may be identifying a policy group based on a device attribute..")

Regarding claim 15, See, Nessett, Curie and Ji combined describe all limitations set forth in claim 14. See further describes:

[port configuration logic] to configure a port module of a switching device with one or more packet rules according to at least one of the service abstractions (paragraph 22, "According to one embodiment, the network policies are used to .. disable network ports based on predetermined conditions,")

Regarding claim 17, See, Nessett, Curie and Ji combined describe all limitations set forth in claim 13. See further describes:

a distribution module (fig. 2, policy repository #20) to distribute the one or more service abstractions to one or more network devices residing on the communications network (paragraph 30, "According to one embodiment, the policies relevant to a particular network device 24, 26, 28 are selected based on a role assigned to the device" and paragraph 35, "A rule type may organize policies into role policies").

4. Claims 19-21 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over See in view of Nessett, Curie and Ji, and further in view of Azarmi.

Regarding claim 19, See, Nessett, Curie and Ji combined describe all limitations set forth in claim 13, where the user is an authenticated user (Curie, col. 17, lines 16-18).

See, Nessett, Curie and Ji combined lack what Azarmi describes:

A role editing module (Nessett, fig. 1, front end #31) to create one or more role abstractions (feature-describing data set), each role abstraction representing a role of a user with respect to the communications network (manageable aspect of the communications network), and each role abstraction including a set of one more service abstractions (management rule profiles) (col. 2, lines 42-51).

It would have been obvious to one with ordinary skill in the art at the time of invention by applicant to specify (another) role abstraction layer to group the (existing) service abstraction layer. The motivation being that "It defines a structural architecture within which business processes, and therefore management systems required to provide services on a network", Azarmi, col. 2, lines 10-12.

Regarding claim 20, See, Nessett, Curie, Ji and Azarmi combined describe all limitations set forth in claim 19. See, Nessett, Curie, Ji and Azarmi further describe:

[logic to] configure a network device with one or more packet rules according to one of the role abstractions (See, paragraph 26, "The policy repository 22 stores a plurality of policy rules that may be used by the network devices 24, 26, 28 to control different network elements" and See, paragraph 38, "The action 58 may be identifying a

policy group based on a device attribute.." *where the policy group [i.e. service abstraction layer] is replaced by Azarmi's feature set [i.e. role abstraction layer]*).

Regarding claim 21, See, Nessett, Curie, Ji and Azarmi combined describe all limitations set forth in claim 20. See, Nessett, Curie, Ji and Azarmi further describe:

[port configuration logic to] configure a port module of a switching device with one or more packet rules according to one of the role abstractions (See, paragraph 22, "According to one embodiment, the network policies are used to .. disable network ports based on predetermined conditions", *where the policy (group) [i.e. service abstraction layer] is replaced by Azarmi's feature set [i.e. role abstraction layer]*).

Regarding claim 23, See, Nessett, Curie, Ji and Azarmi combined describe all limitations set forth in claim 19. See, Nessett, Curie, Ji and Azarmi further describe:

a distribution module (See, fig. 2, policy repository #20) to distribute the one or more role abstractions to one or more network devices residing on the communications network (See, paragraph 30, "According to one embodiment, the policies relevant to a particular network device 24, 26, 28 are selected based on a role assigned to the device" and See, paragraph 35, "A rule type may organize policies into role policies", *where the role (policy) [i.e. service abstraction layer] is replaced by Azarmi's feature set [i.e. role abstraction layer]*).

5. Claims 33-35, 37 and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over See in view of Azarmi, Nessett and Curie and Ji.

Regarding claims 33, See describes a system of controlling usage of network resources on a communication network (abstract, individual network device each distributively performing rules/policy management), [official notice taken that the system may be implemented using a computer comprising a readable medium and a program with instructions which executes the process], comprising:

creating one or more packet rules (policy rules) for analyzing packets received at one or more devices of the communication network, each rule including a condition and action to be taken if a packet received at a device satisfies the condition (fig. 4 and paragraph 35);

storage means for storing one or more created packet rules (paragraph 53, repository table storing the policy (packet) rules);

See lacks what Azarmi describes:

creating one or more role abstractions (feature-describing data set), each role abstraction representing a role of a user with respect to the communications network (manageable aspect of the communications network), and each role abstraction including a set of one more packet rule (management rule profiles containing management rules) (col. 2, lines 42-51, & fig. 20 where such control/provisioning is for [associated with] individual users).

It would have been obvious to one with ordinary skill in the art at the time of invention by applicant to specify the role abstraction layer to group the packet rules (layer). The motivation being that "It defines a structural architecture within which

business processes, and therefore management systems required to provide services on a network", Azarmi, col. 2, lines 10-12.

See and Azarmi combined lack what Nessett describes:

a rule editing module [to create pack rules] (fig. 1, security policy management back-end #32) and a role editing module (Nessett, fig. 1, front end #31) [means to create role abstractions].

It would have been obvious to one with ordinary skill in the art at the time of invention by applicant to specify respective editing modules to be used for creating the packet rules and service abstractions as specified in See and Azarmi. The motivation for using separate modules in performing layered rules & service abstraction functionality is "As the partitioning becomes finer grained, access to resources outside of the firewall partition experiences increasing degraded performance. Another approach to this problem is to distribute firewall functionality down into lower layers of the protocol hierarchy" (Nessett, col. 2, lines 51-56).

See, Azarmi and Nessett combined fails to describe:

controlling usage based on the identity of an authenticated user, and associating one or more service abstraction with an authenticated user.

Curie describes:

controlling usage based on the identity of an authenticated user, and associating one or more service abstraction with an authenticated user to control network resource usage by the authenticated user (abstract, fig. 11A, col. 11, lines 50-52 & col. 17, lines

16-18, user authentication, plus col. 21, lines 50-65, associating/grouping common policy (abstraction) with the user so that the user can use the network resources).

It would have been obvious to one with ordinary skill in the art at the time of invention by applicant to describe an authenticated user is used for controlling network usage and is associated with an service abstraction as described in Curie for the network usage control of See, Azarmi and Nessett.

The motivation for combining the teachings is that it enables the resource provisioning of plurality of organizations (with different users) using a single, centralized logical server (Curie, col. 3, lines 41-57).

Curie further describes the compatible means of creating service abstractions in response to a user (col. 1, lines 52-60, in response to a new user, setting up the resources of such role).

See, Azarmi, Nessett and Curie combined fail to explicitly describe:

wherein one or more packet rules are defined to examine any portion of a packet.

Ji describes packet classification comprising:

wherein one or more packet rules are defined to examine any portion of a packet (abstract, employs bitmaps to classify any field (portion) of an incoming packet).

Ji also describes manually (in response to a user) setting up rules (col. 15, lines 35-38).

It would have been obvious to one with ordinary skill in the art at the time of invention by application to modify the packet classification of See and Curie combined such that the packet rules can examine any portion of a packet as in Ji.

The motivation for combining the teachings is that it results in a high performance packet classification solution that provides an optimal tradeoff between performance and memory size (Ji, col. 4, lines 20-22).

Regarding claim 34, See, Nessett, Azarmi, Curie and Ji combined describe all limitations set forth in claim 33. See, Nessett, Azarmi, Curie and Ji further describe:

[logic to] configure a network device of the communications network with one or more packet rules according to one of the role abstractions (See, paragraph 26, "The policy repository 22 stores a plurality of policy rules that may be used by the network devices 24, 26, 28 to control different network elements" and See, paragraph 38, "The action 58 may be identifying a policy group based on a device attribute.." *where the policy group [i.e. service abstraction layer] is replaced by Azarmi's feature set [i.e. role abstraction layer]*).

Regarding claim 35, See, Nessett, Azarmi, Curie and Ji combined describe all limitations set forth in claim 34. See, Nessett, Azarmi, Curie and Ji further describe step (C) of:

[port configuration logic] to configure a port module of a switching device of the communications network with one or more packet rules according to at least one of the role abstractions (See, paragraph 22, "According to one embodiment, the network policies are used to .. disable network ports based on predetermined conditions", *where the policy (group) [i.e. service abstraction layer] is replaced by Azarmi's feature set [i.e. role abstraction layer]*).

Regarding claim 37, See, Nessett, Azarmi, Curie and Ji combined describe all limitations set forth in claim 33. See, Nessett, Azarmi, Curie and Ji further describe step (C) of:

a distribution module (See, fig. 2, #20) to distribute one or more role abstractions to one or more network devices residing on the communications network (See, paragraph 30, "According to one embodiment, the policies relevant to a particular network device 24, 26, 28 are selected based on a role assigned to the device" and See, paragraph 35, "A rule type may organize policies into role policies", *where the role (policy) [i.e. service abstraction layer] is replaced by Azarmi's feature set [i.e. role abstraction layer]*).

Regarding claims 40, See describes a system of controlling usage of network resources on a communication network (abstract, individual network device each distributively performing rules/policy management), [official notice taken that the system may be implemented using a computer comprising a readable medium and a program with instructions which executes the process], comprising:

creating one or more packet rules (policy rules) for analyzing packets received at one or more devices of the communication network, each rule including a condition and action to be taken if a packet received at a device satisfies the condition (fig. 4 and paragraph 35);

storage means for storing one or more created packet rules (paragraph 53, repository table storing the policy (packet) rules);

See lacks describing a computer program product to perform the above-mentioned system, comprising:

a computer readable medium and computer readable signals stored on the computer readable medium that define instructions that, as a result of being executed by a computer, instruct the computer to perform the process.

The examiner takes official notice that the system of See may be implemented using a computer comprising a readable medium and a program with instructions which executes the process. The motivation being that such implementation using a [generic] computer may be more economical and faster to develop than via a customized hardware system.

See lacks what Azarmi describes:

creating one or more role abstractions (feature-describing data set), each role abstraction representing a role of a user with respect to the communications network (manageable aspect of the communications network), and each role abstraction including a set of one more packet rule (management rule profiles containing management rules) (col. 2, lines 42-51, & fig. 20 where such control/provisioning is for [associated with] individual users).

It would have been obvious to one with ordinary skill in the art at the time of invention by applicant to specify the role abstraction layer to group the packet rules (layer). The motivation being that "It defines a structural architecture within which business processes, and therefore management systems required to provide services on a network", Azarmi, col. 2, lines 10-12.

See and Azarmi combined lack what Nessett describes:

a rule editing module [to create pack rules] (fig. 1, security policy management back-end #32) and a role editing module (Nessett, fig. 1, front end #31) [means to create role abstractions].

It would have been obvious to one with ordinary skill in the art at the time of invention by applicant to specify respective editing modules to be used for creating the packet rules and service abstractions as specified in See and Azarmi. The motivation for using separate modules in performing layered rules & service abstraction functionality is "As the partitioning becomes finer grained, access to resources outside of the firewall partition experiences increasing degraded performance. Another approach to this problem is to distribute firewall functionality down into lower layers of the protocol hierarchy" (Nessett, col. 2, lines 51-56).

See, Azarmi and Nessett combined fails to describe:

controlling usage based on the identity of an authenticated user, and associating one or more service abstraction with an authenticated user.

Curie describes:

controlling usage based on the identity of an authenticated user, and associating one or more service abstraction with an authenticated user to control network resource usage by the authenticated user (abstract, fig. 11A, col. 11, lines 50-52 & col. 17, lines 16-18, user authentication, plus col. 21, lines 50-65, associating/grouping common policy (abstraction) with the user so that the user can use the network resources).

It would have been obvious to one with ordinary skill in the art at the time of invention by applicant to describe an authenticated user is used for controlling network usage and is associated with an service abstraction as described in Curie for the network usage control of See, Azarmi and Nessett.

The motivation for combining the teachings is that it enables the resource provisioning of plurality of organizations (with different users) using a single, centralized logical server (Curie, col. 3, lines 41-57).

Curie further describes the compatible means of creating service abstractions in response to a user (col. 1, lines 52-60, in response to a new user, setting up the resources of such role).

See, Azarmi, Nessett and Curie combined fail to explicitly describe:

wherein one or more packet rules are defined to examine any portion of a packet.

Ji describes packet classification comprising:

wherein one or more packet rules are defined to examine any portion of a packet (abstract, employs bitmaps to classify any field (portion) of an incoming packet).

Ji also describes manually (in response to a user) setting up rules (col. 15, lines 35-38).

It would have been obvious to one with ordinary skill in the art at the time of invention by application to modify the packet classification of See and Curie combined such that the packet rules can examine any portion of a packet as in Ji.

The motivation for combining the teachings is that it results in a high performance packet classification solution that provides an optimal tradeoff between performance and memory size (Ji, col. 4, lines 20-22).

Response to Arguments

6. Applicant's arguments with respect to claims 1-3, 5, 7-9, 11, 13-15, 17, 19-21, 23, 26-29, 31, 33-35, 37 and 40 have been considered but are moot in view of the new ground(s) of rejection.

The examiner is aware that the computer readable signals in claims 26 and 40, also recited on p. 20 of the instant application's specifications, are in reference to instructions stored in the computer readable medium.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure: Boden (US 2001/0000193) describing a fast IP packet filtering method, Pelissier (US 6,850,513) describing a table-based classification, Van Lunteren (US 7,193,997) describing parallel packet classification, Iyer (US 7,136,926) describing a high-speed network rule processing and Li (US 7,154,888) describing a multi-class structure for classifying packets.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to WARNER WONG whose telephone number is (571)272-8197. The examiner can normally be reached on 6:30AM - 3:00PM, M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kwang Yao can be reached on 571-272-3182. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Warner Wong
Primary Examiner
Art Unit 2616

/Warner Wong/
Primary Examiner, Art Unit 2616

/Kwang B. Yao/
Supervisory Patent Examiner, Art Unit 2616